8

9 10

11

12

13

1

5

What is Claimed:

A method for calculating a greatest common divisor of a first binary integer, V, and a second binary integer, V, the method comprising the steps of:

- a) selecting 2M most significant bits of U as a first value U_{2M} and selecting 2M corresponding bits of V as a second value V_{2M}, dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;
 - b) determining a value T as U minus the quantity Q times V;
 - c) if T is less than zero, applying a correction term to Q to obtain a corrected value Q' and assigning the new value for T as U minus the quantity Q' times V;
 - d) assigning V to U and T to V; and
 - e) repeating steps a) through e) until V equals zero, whereby the value remaining in U is the greatest common divisor of the first and second binary integers.
 - 2. A method according to claim 1, wherein:
- step c) includes the step of selecting 2M most significant non-zero bits of T to define a value T_{2M} , wherein the step of applying the correction term is given by the equation:

$$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1);$$
 and

step c) further includes the step of calculating Q", a further corrected value for Q, as the greatest integer less than the quantity V divided by V if the new value of T is less than zero.

1 .	
1-7	3. A method according to claim 1, wherein the first binary integer,
2	U, has a most significant non-zero bit at bit-position B1 and the second binary integer,
3	V, has a most significant non-zero bit at bit-position B2, where B1 and B2 are integers
4	and B1 is greater than B2, the method further including the steps of:
5	subtracting B2 from B1 to obtain a difference value D;
6	comparing \dot{D} to a predetermined threshold value wherein steps a)
7	through d) are performed only if D is greater than a predetermined threshold value;
8	if D is not greater than the predetermined threshold, then, before step e)
9	performing the steps of:
10	determining values X and Y such that U _{2M} times X plus V _{2M} times
11	Y is less than 2^{M} ;
12	assigning a new value to U as U times X plus Y times V; and
13	switching the values of U and V.
1	4. A method according to claim 3, wherein the step of determining
2	values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^{M} , includes the
3	step of invoking a further GCD routine.
1	5. A method according to claim 4 wherein 2M equals 32 and the
2	further GCD routine is a Euclid routine having a modified termination condition.
	a modified termination condition.
1	6. A method according to claim 4, wherein 2M equals 64 and the
2	further GCD routine is a Lehmer routine having a modified termination condition.
1	7. A method according to claim 1, further including a method for
2	calculating a value V-1 being the inverse of V modulo U, wherein:



	1. K
3	step a) further includes the steps of assigning a value of zero to a
4	temporary variable U2 and assigning a value of one to a temporary variable V2; and
5	step d further includes the steps of determining a value T2 as U2 minus
6	Q times V2, assigning the value in V2 to U2 and assigning the value T2 to V2;
7	whereby, at step e) when V equals zero, the value of U2 is V^{-1} .
1	8. A method according to claim 3, further including a method for
2	calculating a value V ⁻¹ being the inverse of V modulo U, wherein:
3	step a) further includes the steps of assigning a value of zero to a
4	temporary variable U2 and assigning a value of one to a temporary variable V2; and
5	step d) further includes the steps of determining a value T2 as U2 minus
6	Q times V2, assigning the value in V2 to U2 and assigning the value T2 to V2;
7	the step of assigning a new value to U as U times X plus Y times V,
8	further includes the step of determining the value T2 as X times U2 plus Y times V2;
9	and
10	the step of switching the values of U and V further includes the step of
11	assigning the value of V2 to U2 and assigning the value T2 to V2;
12	whereby, at step e), when V equals zero, the value of U2 is V ⁻¹ .
1	9. A method for defining a Finite field that includes encryption keys
2	for an encryption algorithm, comprising the steps of:
3	a) selecting a first binary integer value, P, having a number of bits such
4	that the Finite field defined as values ranging between zero and the first value are
5	sufficient for the encryption algorithm to be secure;
6	b) determining if P is a prime number, comprising the steps of

	. ^
	Wh (
7	calculating a greatest common divisor of P, and a second binary integer
8	V, wherein V is a product of predetermined prime numbers, including the steps of:
9	(b1) assigning P to a temporary variable U;
10	
10	b2) selecting 2M most significant non-zero bits of U as a first
11	value U_{2M} and selecting 2M corresponding bits of V as a second value V_{2M} ,
12	dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;
13	b3) determining a value T as U minus the quantity Q times V;
14	b4) if T is less than zero, applying a correction term to Q to
15	obtain a corrected value Q and assigning the new value for T as U minus the
16	quantity Q' times V;
17	b5) assigning V to U and T to V; and
18	b6) repeating steps a) through e) until V equals zero, whereby the
19	value remaining in U is the greatest common divisor of the first and second
20	binary integers;
21	c) if U is greater than one, selecting an other value for P and repeating
22	steps b) through c) until U is equal to one;
23	d) when U is equal to one after step (x), passing P to a probabilistic
24	primality testing routine to determine if P is prime;
25	whereby when P is prime, the integers from 0 to P define the Finite
26	field.
1	10. A method according to claim 9, wherein:

6

7

8

1

2

3

4

5

6

7

8

9

10

11

12

13

step b4) includes the step of selecting 2M most significant non-zero bits of T to define a value T_{2M} , wherein the step of applying the correction term is given by the equation:

$$Q' = Q - (LT_{2M} / V_{2M} \rfloor + 1)$$
; and

step c) further includes the step of calculating Q", a further corrected value for Q, as the greatest integer less than the quantity U divided by V if the new value of T is less than zero.

11. A method according to claim 10, wherein the first binary integer, U, has a most significant non-zero bit at bit-position B1 and the second binary integer, V, has a most significant non-zero bit at bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method further including the steps of:

subtracting B2 from B1 to obtain a difference value D;

comparing D to a predetermined threshold value wherein steps a) through d) are performed only if D is greater than a predetermined threshold value;

if D is not greater than the predetermined threshold, then, before step e) performing the steps of:

determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^{M} ;

assigning a new value to U as U times X plus Y times V; and

switching the values of U and V; and

after step e) if U is greater than 1, further processing U to remove spurious factors.

	1 pt 1
1	A method according to claim 11, wherein the step of determining
2	values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^{M} , includes the
3	step of invoking a further GCD routine.
1	13. A method according to claim 12, wherein 2M equals 32 and the
2	further GCD routine is a Euclid routine having a modified termination condition.
1	14. A method according to claim 12, wherein 2M equals 64 and the
2	further GCD routine is a Lehmer GCD routine having a modified termination
3	condition.
1	15. A method for identifying an encryption value in a Finite field, F _P ,
2	where P is a prime number, based on a private key PV and a received public key PB,
3	comprising the steps of:
4	determining a mathematical inverse of PB modulo P by performing the
5	steps of:
6	a) assigning P to a temporary variable U and assigning PB to a
7	temporary variable V and assigning a value of zero to a temporary variable U2
8	and assigning a value of one to a temporary variable V2;
	y and the second to a temporary variable v2,
9	b) selecting 2M most significant bits of U as a first value U _{2M} and
10	selecting 2M most significant bits of V as a second value V_{2M} , dividing U_{2M} by
11	V_{2M} and storing an integer portion of the result as a value Q;
	2M and value Q,
12	c) determining a value T as U minus the quantity Q times V;
	of descriming a value I as o minus the qualitity Q times V,
3	d) if T is less than zero, applying a correction term to Q to obtain
4	a corrected value Q' and assigning the new value for T as U minus the quantity
5	Q' times V;

performing the steps of:

è) determining a value T2 as U2 minus Q times V2, assigning the 16 value in V2 to U2, assigning the value T2 to U2, assigning V to U and T to V; 17 and 18 f) repeating steps a) through e) until V equals zero, whereby the 19 value remaining in U2 is the mathematical inverse of PB; and 20 dividing PV by PB modulo P by multiplying PV times the mathematical 21 inverse of PB, wherein the result is the encryption value. 22 A method according to claim 15, wherein: 1 16. step d) includes the step of selecting 2M most significant bits of T to 2 define a value T_M, wherein the step of applying the correction term is given by the 3 4 equation: $Q' = Q - (T_{2M} \setminus V_{2M} \rfloor + 1)$; and 5 step d) further includes the step of calculating Q", a further corrected 6 value for Q, as the greatest integer less than the quantity U divided by V if the new 7 value of T is less than zero. 8 A method according to claim 15, wherein the variable U has a 1 17. most significant bit at bit-position B1 and the variable V has a most significant bit at 2 bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method 3 4 further including the steps of: subtracting B2 from B1 to obtain a difference value D; 5 comparing D to a predetermined threshold value wherein steps a) 6

through d) are performed only if D is greater than a predetermined threshold value;

if D is not greater than the predetermined threshold, then, before step e)

determining values X and Y such that U_{2M} times X plus V_{2M} 10 times Y is less than 2^M; 11 assigning a new value to U as U times X plus Y times V and 12 determining the value T2 as X times U2 plus Y times V2; and 13 switching the values of U and V and assigning the value of V2 to 14 U2 and assigning the value T2 to U2. 15 A method according to claim 17, wherein the step of determining 1 18. values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^{M} , includes the 2 step of invoking a further GCD routine. 3 A method according to claim 17, wherein 2M equals 32 and the 1 19. further GCD routine is a Euclid routine having a modified termination condition. 2 A method according to claim 17, wherein 2M equals 64 and the 20. 1

further GCD routine is a Lehmer routine having a modified termination condition.